The internet's long war

Flawed internet security means that Sony, Twitter, the US Senate and the CIA have all been hacked in recent months

Is hacking getting more serious?
No question. In April, Sony revealed that it had suffered the largest theft of personal data in history. The names, addresses, dates of birth and passwords of 77 million people (including 3 million Britons) had been stolen from a network that allows Sony customers to play computer games against each other on the internet. This haul of information, which could theoretically be used to launch countless crimes, was the latest booty in an escalating conflict between hackers and some of the world's best-known companies and institutions. Since 2007, victims have included the Royal Bank of Scotland, Visa, Mastercard, Paypal, Google, Lockheed Martin, the CIA, the US Senate, the NHS and hence, by extension, millions of us.

A member of Anonymous at a demonstration in San Francisco

Why are these attacks on the increase?
In large part, the story of hacking is of a war between legitimate programmers and their bedroom-based foes – tricksters and vandals – that dates from the first days of the personal computer in the 1980s (see box). But in recent years, two important shifts have occurred. One is the increasing ability of hackers to make money through their crimes, either by stealing people's identity or by luring us to fraudulent schemes through emails and pop-up ads; the other is the involvement of state-sponsored hackers and new kinds of quasi-political, anarchic groups.

Which governments are involved?
A report just published by McAfee, the largest security technology company in the world, reveals that over the past five years, one country has systematically hacked its way into the computer systems of 72 corporations and government agencies in the US, UK and elsewhere. These include the Olympic's anti-doping agency, which was targeted just before and after the Beijing Games, confirming suspicions that the country in question was China – earlier this year China was found to have penetrated the Foreign Office's internal communications system. But China is only the worst offender: a host of other countries and companies engage in similar enterprises. "I divide the entire Fortune Global 2000 firms into two categories: those that know they've been compromised and those that don't know yet," security analyst Rik Ferguson told The Guardian.
Throw organised crime and industrial-scale production of viruses in Russia and China into the mix, and it is no surprise that the UK classifies cyber-crime as the nation's second-biggest national security threat after terrorism.

How do hackers operate?
Depends what they're after. One tool, though, is "malware" – short for malicious software. These programmes are often disguised as something useful (when they're known as "Trojans") or as email attachments. In 2008 internet security company Symantec calculated that malware was now being produced in greater quantities than legitimate software. Some programmes, like those that make a mess of your hard drive, are merely irritating – others are ominous. "Screen-scrapers" and "keystroke-loggers", for example, record everything you type and look at, and send it to a hacker. Other malware turns your PC into a "zombie machine" entirely under the control of a fraudster, thousands of miles away.

What about anti-virus software?
Microsoft, Google and Apple strive to keep ahead of the hackers, but the truth is that malware and "phishing" (in which cleverly disguised emails try to coax personal information from you) are just part of the story. The cybercriminals are after your personal data (passwords, credit-card numbers, names, addresses – the building blocks of your online identity), and these details can be obtained in any number of ways. Last year a software developer in Seattle wrote a programme called Firesheep to show how easy it is for hackers to sit in a café and steal personal information from the people around them surfing the net on their phones and laptops. We're all vulnerable. Last September, the head of Interpol, Ronald Noble, realised hackers had stolen his identity to find out about an upcoming police operation.

What are hackers out to get?
Most want money. There's a huge black market for personal data, with higher prices for credit-card numbers or passwords known to work. In November 2008, hackers spent just over £5m in 12 hours with information stolen from RBS Worldpay, a payment system used by the Royal Bank of Scotland. But in truth there is a galaxy of motives for hackers: from the criminal, to the political (such as Google's repeated targeting by Chinese hackers) to the ideological. This last includes a mixture of anarchism and anti-capitalism, and drives groups from Julian Assange's WikiLeaks to the even more mysterious "Anonymous". Anonymous, and its splinter group, "LulzSec", carried out sympathy attacks for WikiLeaks earlier this year, as well as their own disruptions of Spain's electoral commission and the CIA, by directing millions of machines to their websites, crippling their servers.

How worried should we be by identity theft/cybercrime?
It has cost us £27bn this year alone, so it's not a trivial matter. The UK has committed £650m to fight "e-crime", and last month helped to set up the International Cybercrime Security Protection Alliance, which will seek to unify public and private-sector approaches to the problem. For individuals, however, the threat can be exaggerated. In the Sony case, customers' credit-card details were encrypted and kept separate from the rest of their data, making any direct identity theft hard to carry out. The greater danger posed by cybercrime is more subtle. The beauty and power of the internet lies in its ability to operate without restraints: its foundations are built on trust. Hackers undermine that trust, and the raft of security measures that may be set up in the war against them could start to block the free flow of information. "The Internet," as The New York Times puts it, "is getting scary."

Origins of the malware plague

According to The Observer, the global malware epidemic began in 1971 in Boston, at the desk of a programmer called Bob Thomas, who was working on Arpanet, a prototype for the internet. Thomas released an experimental programme that would replicate itself around the network, displaying a message as it went: "I'm the creeper, catch me if you can!" Soon someone did, creating "The Reaper" which chased and deleted it. But an idea was born.

In 1988, Robert Morris, a researcher at Cornell University, released a "worm" that he hoped would tell him how many computers were connected to the internet. But the worm began reproducing and got out of control, and Morris was arrested. The first common viruses were pranks spread by floppy disk. One, Melissa (named after a stripper), caused $80m of damage. In the 1990s, the rise of the internet and the success of Windows 95 created overwhelming temptations for criminal hackers. Last year Albert Gonzalez, an American fraudster, was sentenced to 20 years in prison for stealing the details of 130 million credit cards.